SECURITY FOR ONE EXCHANGE WITH TWO SIDES

Doreen Espinoza

UHIN, Chief Business Development and Privacy Officer

TO BE OR NOT TO BA

- The original Security rule designated the Clearinghouse as a Covered Entity. This was not changed with the publication of the OMNIBUS
- The original rule Security rule did not name a Health Information Exchange as a covered entity. This was changed in the OMNIBUS. the HIE is now a Business Associate.

DIFFERENT MISSIONS

- Clearinghouse:
  - to send and receive data as is
  - to transform data from non-standard to standard
  - data available for the customer it belongs to
- HIE
  - To share data for treatment - combine
  - To share data as requested by patients with treating providers, health insurers and government i.e. public health

NOT THE SAME DATA ANIMAL

- Different types of healthcare data
  - Administrative Transactions
    - Financial
    - Claim
    - Benefits
  - Clinical Data
    - Results
    - Notes
    - Medications
- Different types of access/roles
  - Office Staff – Office Manager, billing clerk, front desk
  - Clinical Personnel – Doctors, Nurses, Pharmacists
- Different Usage
  - Work flow
  - Storage - volume
  - Retrieval – time sensitivity

SECURITY CONCERNS

- Risk analysis
  - Roles – for internal staffs and customers
  - Access – Amount of Access – types of access
- Security for access
    - Sign up process
      - Authentication
      - Attestation
- Security for storage and retrieval – who has it and where is it???
    - Transactions can be stored a the end of the pipelines or at the clearinghouse
    - Clinical data is stored federated, at central repository or at a third party
- Non-repudiation
  - Resubmit a corrected transaction
  - Clinical data must be able to show who, what, and when something was changed
- Data encryption
    - In transit, at rest and in archive

HOW TO ADDRESS

- Treat all data according to the sensitivity and risk that it implies
- Mitigate your risk by:
  - training,
  - having your agreements well spelled out
  - meeting the minimum security requirement spelled out by NIST and
  - make sure your business associates are in compliance